Internet Application Development Guidance for Medicare Fiscal Intermediaries and Carriers

Background

The Center for Medicare & Medicaid Services (CMS) has developed architectural, security and database standards for Internet-facing infrastructure to house CMS applications in support of the Agency's goals and services. This document addresses requirements for Fiscal Intermediaries and Carriers as they develop and implement Internet-facing applications to extend their services to beneficiaries within the scope of providing claims status and eligibility information.

Architecture Requirements

- Compliance with CMS Internet Architecture (including Minimum Platform Security Requirements) to establish a secure infrastructure for hosting an Internet-facing application.
  http://www.cms.hhs.gov/it/enterprisearchitecture/internetarch.pdf

- Compliance with CMS Target Architecture as it pertains to principles of the "good enough" architecture and product selection for the operational environment. At a minimum, the platform must be Unix-based Sun Solaris and use Java, including Java 2 Platform Enterprise Edition (J2EE), as development and management platform. Refer to the J2EE Application Development Guidelines, as published by CMS:
  http://www.cms.hhs.gov/it/enterprisearchitecture/cms_target_architecture.pdf
  http://www.cms.hhs.gov/it/enterprisearchitecture/J2EE_Application_Development_Guidelines.pdf

- Use resources to leverage existing technology and solutions, when possible, such as platform and software developed by contractors and in compliance with CMS standards to meet the same or similar business requirements. The technology and solutions would also have to align with requirements for the Medicare Administrative Contractors (MAC), Enterprise Data Centers (EDC), and Standard Front-End (SFE) initiatives.

- Use the Internet Gateway hosted at CMS' Web Hosting site to route all application traffic through it to better monitor and manage network traffic associated with these solutions. This requires an IP-based network connection to the Medicare Data Communications Network's (MDCN).

Security Requirements

- Address all major findings resulting from security audit/evaluations, to include: 1) Chief Financial Officer (CFO) and EDP Audits; 2) SAS 70 Internal Control Review; 3) System Security Self-Assessment, as required by the Federal

Information Security Management Act of 2002 (FISMA) and delineated in the Contractor Assessment Security Tool (CAST); and 4) tests and evaluations conducted pursuant to Section 912 of the Medicare Prescription Drug, Improvement and Modernization Act of 2003 (MMA).

- Compliance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-41, Guidelines on Firewalls and Firewall Policy, and NIST SP 800-42, Guideline on Network Security Testing.

- Compliance with security best practices, such as the CMS Acceptable Risk Safeguards and other security documentation, as published by CMS: http://cms.hhs.gov/it/security/docs/ars.pdf

- Certification and accreditation (C&A) of the Internet-facing applications including platform systems housing the applications. C&A dependent on the completion of the Information Security (IS) Business Risk Assessment (RA), to include business roles; and the Information Security System Security Plan (SSP) and Risk Assessment (RA) for the infrastructure, platform and applications. The IS RA must address e-Authentication requirements and controls for electronic transactions, or refer to a separate document, if one exists.

  Certification and accreditation must be completed prior to production implementation. The SSP and RA must be developed according to CMS Methodologies and follow the SSP/RA Guidance Document: http://www.cms.hhs.gov/it/security/docs/ssp_meth.pdf http://www.cms.hhs.gov/it/security/docs/RA_meth.pdf

- Security testing/evaluation must be performed by a CMS-contracted third-party to review security controls of the platform and application, and processes supporting the system's configuration and change management. Fiscal Intermediaries and Carriers provide CMS with system documentation within 10 working days of being notified by the Center for Medicare Management (CMM) of penetration testing and security assessment timeframe.

Enterprise Data Interchange Requirements

- The application will use HIPAA standards for claim status (276/277) and eligibility (270/271).

- Applications must return consistent data responses. For example, queries and data access methods such as Interactive Voice Recognition (IVR), Direct Data Entry (DDE), and computer-to-computer need to return consistent data content regardless of the method used.

Privacy Requirements

- Applications must complete a Privacy Impact Assessment in accordance with Section 208 of the E-Government Act. This requirement is for an assessment when authentication technology is added to an electronic information system accessed by members for the public. See OMB Memorandum M-03-22 for guidance.

- An assessment must be completed to ensure the disclosure of information is made according to an approved routine use set forth in the Systems of Records Notice published in the Federal Register.

Evaluation and Performance Metrics

During the pilot, analysis will be performed to assess the impact on business operations. The following metrics will be performed and reported to CMM on a regular basis:

1. Provider Authentication

The contractor shall submit a summary that will provide CMS with the following information:

- Authentication method used – advantages and disadvantages of chosen method
- Effect on participating providers – timeliness of process, include any provider feedback
- Effectiveness of security measures through the analysis of audit trail, Intrusion Detection software, and firewall logs.
- Lessons Learned

2. Provider Registration/Enrollment

The contractor shall submit a report that will provide information on providers participating in pilot. The report should include but is not limited to:

- Demographic profiles on who is using the application
- Provider feedback on web enrollment process
- Lessons learned

3. Provider Inquiries for Beneficiary Eligibility/Claims Status

The contractor shall submit a monthly summary report to help CMS better understand:

- The length, subject, and number of Internet inquiries for eligibility and claim status.
- The reason for inquiry information not being returned to the provider and the frequency of the occurrence per user.

4. Web Usage

   The contractor shall submit a monthly summary report to provide information on:

   - Who specifically is using the web site
   - What is the frequency and duration of site usage
   - How often the Web site is accessed after "business hours"

5. Customer Service/Technical Support

   The contractor shall submit a monthly summary report that shows:

   - The number and length of times the web site was unavailable
   - The response time of the application for specific browser and operating systems or the impact on mainframe capacity.
   - The number of calls regarding the web site

6. Post-Pilot Analysis

   After the sixth month of the pilot, analysis will be performed and various reports provided that:

   - Track the cost of the pilot (estimated vs. actual cost)
   - Estimate of savings (cost/benefit analysis)
   - Report on the effects of the pilot on pre data.